

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité 2010-34

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-034>

---

### Gestion du document

Référence	CERTA-2010-ACT-034
Titre	Bulletin d'actualité 2010-34
Date de la première version	26 août 2010
Date de la dernière version	–
Source(s)	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-034.pdf>

Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-034/>

## 1 Un filtre ralentit le traitement d'incident

Cette semaine, le CERTA et l'un de ses correspondants ont constaté un effet pervers d'un filtre dont le but initial est de protéger le réseau de l'administration en question.

L'été rend les correspondants du CERTA moins disponibles. En congés ou occupés à suppléer des absents, ils ne peuvent répondre immédiatement au téléphone. La messagerie électronique, par son caractère asynchrone, offre la possibilité de déposer un message et de transmettre un contenu technique.

En l'espèce, les non-réponses téléphoniques ont conduit le CERTA à transmettre les informations précises (un lien malveillant inséré sur plusieurs pages d'un site Web), par courriel. Ce courriel ne contenait que du texte brut. Cette information n'est pas parvenue aux destinataires. En effet, un filtre antipourriel détectant dans le corps du message un lien vers un site malveillant « bien connu » aura conclu hâtivement à la nature inopportune du message et l'aura bloqué de manière silencieuse. Une première relance a subi le même sort. Une deuxième relance, rédigée différemment, a réussi à parvenir à un destinataire.

Le résultat de ce blocage est un retard de trois semaines dans le traitement de l'incident.

Ce blocage est connu des correspondants du CERTA pour des fichiers infectés par des virus, qu'il faut encapsuler pour traverser les fourches caudines des passerelles antivirus.

Il faut désormais prendre des précautions supplémentaires pour transmettre des données de nature textuelle. La mise en liste blanche des serveurs SMTP des équipes de traitement d'incident peut éviter les blocages intempestifs par les filtres.

## 2 Mise à jour de sécurité Mac OS X

Lors de la mise à jour de sécurité numéro 2010-005 du 24 août 2010, Apple a corrigé 13 vulnérabilités (cf avis CERTA-2010-AVI-403). Cinq d'entre elles concernaient l'interpréteur de langage *PHP*, embarqué dans la version Serveur de *Mac OS X*, mais aussi dans la version réservée aux ordinateurs personnels. Bien que le serveur Web ne soit pas activé par défaut sur cette dernière, la plus sérieuse de ces failles (CVE-2010-2225) permet une exécution de code arbitraire à distance.

Il est également intéressant de noter que le système d'Apple est vulnérable à des attaques via des fichiers *PDF* malveillants (CVE-2010-1801) pouvant entraîner une exécution de code arbitraire. Toutefois, il s'agit ici bien d'un composant graphique dédié à *Mac OS X* qui a été corrigé et non pas un logiciel d'un développeur tiers. Il convient donc d'être prudent lors de la réception de documents de ce type, même lorsqu'on n'utilise pas de logiciel créé par le créateur du format.

L'application de ce correctif, quoique volumineux, est donc impératif pour rétablir le niveau de sécurité des postes et serveurs utilisant le système d'exploitation d'Apple.

### Documentation

- Avis CERTA-2010-AVI-403 du 25 août 2010 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-403>
- Bulletin de sécurité Apple HT4312 du 24 août 2010 :  
<http://support.apple.com/kb/HT4312>

## 3 Vulnérabilité liée au chargement de DLLs (DLL Hijacking)

Le 23 août dernier, Microsoft a publié un avis de sécurité concernant l'exploitation d'une vulnérabilité dans des applications Windows.

Cette vulnérabilité repose sur la manière dont les applications chargent des bibliothèques dynamiques (DLL) via l'API *LoadLibrary*.

Si une application charge une DLL sans spécifier le chemin (par exemple *LoadLibrary(DLL\_a\_Charger.dll)* au lieu de *LoadLibrary(c:\MonApplication\DLL\_a\_Charger.dll)*), alors l'algorithme utilisé par Windows par défaut commence par vérifier si la DLL se trouve dans le répertoire courant. Si c'est le cas, c'est cette DLL qui sera chargée.

Imaginons le scénario suivant :

- Un attaquant a déposé sur un partage réseau un document qui peut être ouvert par l'application XY ;
- dans le même répertoire se trouve une DLL malveillante (*DLL\_a\_Charger.dll*) dont le nom est identique à une DLL légitime qui est connue pour être chargée par l'application XY ;
- l'utilisateur double-clique sur le document pour l'ouvrir (via l'explorateur de fichiers ou via un lien) ;
- l'ouverture du document va déclencher le chargement de l'application XY qui prend en charge ce type de document ;
- l'application XY ayant besoin de la DLL "*DLL\_a\_Charger.dll*" , elle appelle *LoadLibrary(DLL\_a\_Charger.dll)* ;
- l'API *LoadLibrary* vérifie si le fichier *DLL\_a\_Charger.dll* se trouve dans le répertoire courant (répertoire où se trouve le document à ouvrir) ;
- Le fichier étant bien présent, *LoadLibrary* charge et exécute la DLL malveillante *DLL\_a\_Charger.dll*.

On voit donc qu'il s'agit d'une vulnérabilité concernant la façon dont est appelé *LoadLibrary* par l'application, et non d'une vulnérabilité dans l'API *LoadLibrary* elle-même.

On a vu dans le scénario précédent qu'un document sur un partage réseau (type *SMB*) peut servir de vecteur d'attaque.

A ce vecteur il faut ajouter les partages *WebDav*. *WebDav* est un protocole qui s'appuie sur *HTTP* pour permettre la manipulation de document sur Internet (ouvrir/modifier/... un document).

On peut donc imaginer un scénario dans lequel un attaquant a placé un document et sa DLL malveillante sur un serveur *WebDav* qu'il contrôle. Ensuite par ingénierie sociale (courriel, page Web spécialement construite, etc., il amène l'utilisateur à cliquer sur un lien pour ouvrir ce document. Ouverture qui provoquera le chargement de la DLL malveillante depuis le serveur *WebDav*.

A ce jour des dizaines d'applications (navigateurs, suites bureautique, outils, etc.) sont impactées par cette vulnérabilité.

Dans l'attente des correctifs, le CERTA recommande les contournements suivants :

- Désactiver le service client *WebDav* (*WebClient*) sur les postes de travail (cela peut potentiellement entraîner des effets de bord sur des applications nécessitant ce service, à tester donc) ;
- déployer et configurer la mise à jour Microsoft KB2264107 qui permet, via une nouvelle entrée de registre (*CWDIllegalInDllSearch*), d'interdire le chargement de DLLs depuis un dossier *WebDav* ou un partage réseau *SMB* (effets de bord potentiels aussi dans ce cas, principalement pour les partages réseaux, des tests s'imposent donc aussi ici) ;
- bloquer les ports *tcp/139* et *tcp/445* au niveau des pare-feux périmétriques.

Les proxys / sondes peuvent aussi être configurés pour bloquer les requêtes *WebDav* tentant de charger des fichiers avec l'extension ".dll" (cela ne fonctionnera pas pour les bibliothèques n'ayant pas l'extension .dll).

Cette vulnérabilité applicative peut s'exploiter sur toutes les versions de Windows.

Outre les vecteurs réseaux, l'exploitation peut aussi avoir lieu en local via, par exemple, une clé USB ou encore une archive ZIP contenant le couple document/DLL.

### 3.1 Documentation

- Avis Microsoft #2269637 du 23 août 2010:  
<http://www.microsoft.com/technet/security/advisory/2269637.mspx>
- Article Microsoft KB2264107 :  
<http://support.microsoft.com/kb/2264107>
- Documentation de L'API LoadLibrary :  
<http://msdn.Microsoft.com/en-us/library/ff919712%28VS.85%29.aspx>

## 4 Liens utiles

- Mémento sur les virus :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information du CERTA sur l'acquisition de correctifs :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/>
- Note d'information du CERTA sur les systèmes obsolètes :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/>
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>
- Note d'information du CERTA sur les mots de passe :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>
- Note d'information sur la terminologie d'usage au CERTA :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/>
- Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/>
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :  
<http://www.auscert.org.au/render.html?it=1937>
- Note d'information du CERTA sur les risques associés aux clés USB :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/>
- Note d'information du CERTA sur les outils d'indexation et de recherche :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/>
- Note d'information du CERTA sur la gestion des noms de domaine :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/>
- Note d'information du CERTA sur le bon usage de PHP :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/>

## 5 Rappel des avis émis

Dans la période du 20 au 26 août 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-390 : Multiples vulnérabilités dans IBM Tivoli Storage Manager FastBack
- CERTA-2010-AVI-391 : Vulnérabilité dans le module pam\_xauth
- CERTA-2010-AVI-392 : Vulnérabilité dans le noyau Linux
- CERTA-2010-AVI-393 : Vulnérabilité dans des produits Blue Coat
- CERTA-2010-AVI-394 : Vulnérabilité dans Adobe Acrobat et Reader
- CERTA-2010-AVI-395 : Multiples vulnérabilités dans Google Chrome
- CERTA-2010-AVI-396 : Vulnérabilité dans Novell iPrint Client
- CERTA-2010-AVI-397 : Vulnérabilités dans phpMyAdmin
- CERTA-2010-AVI-398 : Vulnérabilités dans phpCAS
- CERTA-2010-AVI-400 : Multiples vulnérabilités dans Adobe Shockwave Player
- CERTA-2010-AVI-401 : Vulnérabilité dans Xorg
- CERTA-2010-AVI-402 : Vulnérabilités dans Quagga
- CERTA-2010-AVI-403 : Multiples vulnérabilités dans Apple Mac OS X
- CERTA-2010-AVI-404 : Vulnérabilité dans Squid
- CERTA-2010-AVI-405 : Vulnérabilité dans Trend Micro Internet Security Pro 2010
- CERTA-2010-AVI-406 : Vulnérabilité dans AIX ftpd
- CERTA-2010-AVI-407 : Vulnérabilités dans Cisco Unified Communications Manager
- CERTA-2010-AVI-408 : Vulnérabilités dans Cisco Unified Presence

Durant la même période, les avis suivants ont été mis à jour :

- CERTA-2010-AVI-359-001 : Multiples vulnérabilités dans FreeType (ajout du bulletin Ubuntu)
- CERTA-2010-AVI-399-001 : Vulnérabilités dans MySQL (rectification des liens vers les bulletins de l'éditeur)

## 6 Actions suggérées

### 6.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel réglementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

### 6.2 Concevoir une architecture robuste

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en oeuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

### 6.3 Appliquer les correctifs de sécurité

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

## 6.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

## 6.5 Analyser le réseau

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le CERTA peut vous aider dans ce travail d'analyse.

## 6.6 Réagir aux incidents de sécurité

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements inexplicables et d'apparence anodine qui s'avèrent, au cours de l'analyse, être liés à un incident majeur de sécurité. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

## 6.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, l'ANSSI dispose d'un centre de formation :

[http://www.ssi.gouv.fr/site\\_rubrique67.html](http://www.ssi.gouv.fr/site_rubrique67.html)

## 7 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

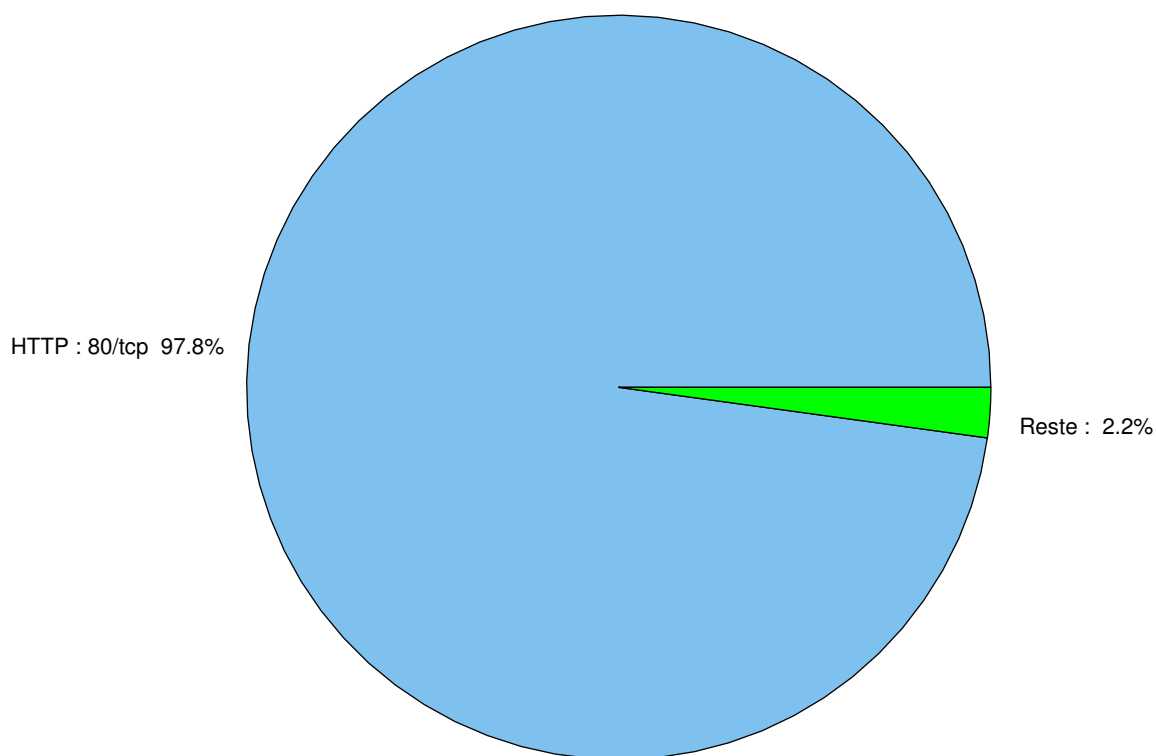


FIG. 1: Répartition relative des ports pour la semaine du 20 au 26 août 2010

Port	Protocole	Service	Porte dérobée	Référence possible CERTA
21	TCP	FTP	–	CERTA-2003-AVI-132 CERTA-2004-AVI-064 CERTA-2004-AVI-066 CERTA-2006-AVI-040
22	TCP	SSH	–	CERTA-2003-AVI-152 CERTA-2006-AVI-100
23	TCP	Telnet	–	CERTA-2003-AVI-209 CERTA-2003-AVI-131 CERTA-2007-ALE-005-001
25	TCP	SMTP	–	CERTA-2006-AVI-124 CERTA-2006-AVI-135
42	TCP	WINS	–	CERTA-2004-AVI-384
69	UDP	IBM Tivoli Provisioning Manager	–	CERTA-2007-AVI-320
80	TCP	HTTP	–	CERTA-2004-AVI-195 CERTA-2004-AVI-239 CERTA-2006-AVI-055 CERTA-2006-AVI-069 CERTA-2006-AVI-156 CERTA-2006-AVI-315
106	TCP	MailSite Email Server	–	– CERTA-2007-AVI-008
111	TCP	Sunrpc-portmapper	–	CERTA-2003-AVI-052
119	TCP	NNTP	–	CERTA-2004-AVI-340
135	TCP	Microsoft RPC	–	CERTA-2003-ALE-002 CERTA-2003-AVI-111 CERTA-2004-AVI-127
137	UDP	NetBios-ns	–	CERTA-2004-AVI-031
139	TCP	NetBios-ssn et samba	–	CERTA-2004-AVI-368

				CERTA-2003-AVI-168 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-213 CERTA-2005-AVI-302 CERTA-2005-AVI-398 CERTA-2006-AVI-283 CERTA-2006-AVI-338 CERTA-2007-AVI-321
143	TCP	IMAP	–	CERTA-2005-AVI-185
389	TCP	LDAP	–	CERTA-2003-AVI-102 CERTA-2003-AVI-068 CERTA-2003-AVI-041 CERTA-2003-AVI-004 CERTA-2004-AVI-126 CERTA-2007-AVI-294
427	TCP	Novell Client	–	CERTA-2006-AVI-538
443	TCP	HTTPS	–	CERTA-2003-AVI-156 CERTA-2004-AVI-126 CERTA-2004-AVI-247 CERTA-2004-AVI-343 CERTA-2007-AVI-153
445	TCP	Microsoft-smb	–	CERTA-2004-AVI-053 CERTA-2003-AVI-105 CERTA-2004-AVI-126 CERTA-2005-AVI-051 CERTA-2005-AVI-302 CERTA-2006-AVI-283 CERTA-2006-AVI-338 CERTA-2007-AVI-321 CERTA-2007-ALE-010
445	UDP	Microsoft-smb	–	CERTA-2007-ALE-010
1023	TCP	–	Serveur ftp de Sasser.E	–
1080	TCP	Wingate	MyDoom.F	CERTA-2006-AVI-232
1433	TCP	MS-SQL-Server	–	CERTA-2002-ALE-006
1434	UDP	MS-SQL-Monitor	–	CERTA-2002-AVI-157
2100	TCP	Oracle XDB FTP	–	CERTA-2005-ALE-002
2381	TCP	HP System Management	–	CERTA-2006-AVI-248
2512	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2513	TCP	Citrix MetaFrame	–	CERTA-2006-AVI-491
2745	TCP	–	Bagle	–
2967	TCP	Symantec Antivirus	Yellow Worm	CERTA-2006-AVI-221
3104	TCP	CA Message Queuing	–	CERTA-2007-AVI-331
3127	TCP	–	MyDoom	–
3128	TCP	Squid	MyDoom	CERTA-2004-AVI-062 CERTA-2004-AVI-186 CERTA-2004-AVI-316 CERTA-2004-AVI-348
3268	TCP	Microsoft Active Directory	–	CERTA-2007-AVI-294
3306	TCP	MySQL	–	–
4899	TCP	Radmin	–	–
5000	TCP	Universal Plug and Play	Bobax, Kibuv	CERTA-2001-AVI-165 CERTA-2006-AVI-212 CERTA-2006-AVI-297
5151	UDP	IPSwitch WS_TP	–	CERTA-2007-AVI-312
5151	TCP	ESRI ArcSDE	–	CERTA-2007-AVI-367
5554	TCP	SGI ESP HTTP	Serveur ftp de Sasser	–

5900	TCP	VNC	-	CERTA-2006-AVI-198 CERTA-2006-AVI-299
6014	TCP	IBM Tivoli Monitoring	-	CERTA-2007-AVI-183
6070	TCP	BrightStor ARCserve/Enterprise Backup	-	CERTA-2005-AVI-293
6101	TCP	Veritas Backup Exec	-	CERTA-2005-AVI-024
6106	TCP	Symantec Backup Exec	-	CERTA-2007-AVI-303
6129	TCP	Dameware Miniremote	-	CERTA-2003-AVI-214 CERTA-2005-AVI-326
6502	TCP	CA BrightStor ARCserve Backup	-	CERTA-2007-AVI-029
6503	TCP	CA BrightStor ARCserve Backup	-	CERTA-2007-AVI-029
6504	TCP	CA BrightStor ARCserve Backup	-	CERTA-2007-AVI-029
8080	TCP	IBM Tivoli Provisioning Manager	-	CERTA-2007-AVI-153
8866	TCP	-	Porte dérobée Bagle.B	-
9898	TCP	-	Porte dérobée Dabber	-
10000	TCP	Webmin, Veritas Backup Exec	-	CERTA-2005-AVI-229 CERTA-2005-AVI-313
10080	TCP	Amanda	MyDoom	-
10110	TCP	IBM Tivoli Monitoring	-	CERTA-2007-AVI-183
10916	TCP	Ingres	-	CERTA-2007-AVI-275-001
10925	TCP	Ingres	-	CERTA-2007-AVI-275-001
12168	TCP	CA eTrust antivirus	-	CERTA-2007-AVI-217
13701	TCP	Veritas NetBackup	-	CERTA-2005-AVI-447
18264	TCP	CheckPoint interface	-	CERTA-2005-AVI-310
54345	TCP	HP Mercury	-	CERTA-2007-AVI-075
65535	UDP	LANDesk Management Suite	-	CERTA-2007-AVI-176

TAB. 2: Correctifs correspondant aux ports destination des paquets rejetés

port	pourcentage
80/tcp	97.84
25/tcp	0.96
1080/tcp	0.3
135/tcp	0.13
2967/tcp	0.12
1433/tcp	0.11
445/tcp	0.1
22/tcp	0.09
1434/udp	0.05
3389/tcp	0.04
3128/tcp	0.03
15118/tcp	0.01

TAB. 3: Paquets rejetés

## Liste des tableaux

1	Gestion du document . . . . .	1
2	Correctifs correspondant aux ports destination des paquets rejetés . . . . .	8
3	Paquets rejetés . . . . .	9

## Gestion détaillée du document

26 août 2010 version initiale.